




**Baker
McKenzie.**

EMEA HR Privacy Newsletter

February 2024



Welcome to the next edition of our quarterly HR Privacy newsletter designed to keep you updated with key cases, enforcement action, legal developments, trends and news relating to employment / HR data privacy matters, which is brought to you by the Baker McKenzie EMEA Employment and Compensation practice group. This edition explores high-profile case-law decisions and new regulations, consultations and guidance in the UK, EU, Germany, Spain, Switzerland, and Saudi Arabia markets.

We hope you find this newsletter useful. We welcome feedback, so please feel free to email [Michael Yeouart](#) with any comments.

Contents

UK	2
In the courts and enforcement action	3
Court of Appeal provides clarity on the UK Information Commissioner's responsibilities in handling complaints lodged by data subjects	3
ICO orders employers to stop using facial recognition technology to monitor attendance of their employees	4
Regulations, consultations and guidance	5
ICO Draft Guidance – Recruitment and selection	5
ICO Draft Guidance – Keeping employment records	7
European Union	9
In the courts	10
Data subject access rights mean access to medical records should be free of charge	10
Germany	12
In the courts	13
No entitlement to compensation for late and incomplete response to DSAR	13
Lack of independence justified removal of works council chair as data protection officer	15
Spain	17
Regulations, consultations and guidance	18
Increased risks with using biometric data in monitoring workplace access and working hours	18
Switzerland	20
Regulations, consultations and guidance	21
A quick look at recent changes to the data protection regime in Switzerland	21
Saudi Arabia	23
Regulations, consultations and guidance	24
New personal data protection law in Saudi Arabia: HR privacy considerations	24

UK



In the courts and enforcement action

Court of Appeal provides clarity on the UK Information Commissioner's responsibilities in handling complaints lodged by data subjects

In brief

In *Delo v Information Commissioner*, the Court of Appeal has given some useful guidance on the UK Information Commissioner's (Commissioner) responsibilities in handling complaints lodged by data subjects.

Facts

Mr Delo made a data subject access request to Wise Payments Limited (Wise) a financial institution that he held an account with. Wise refused to provide some of the information sought by Mr Delo claiming that it was exempt from doing so. He complained to the Commissioner that this response was not compliant with his rights of access. Having reviewed the relevant correspondence between Mr Delo and Wise, the Commissioner advised that it was likely that Wise had complied with its obligations and that the Information Commissioner's Office (ICO) would take no further action against Wise. Mr Delo brought a claim for judicial review and exercised his right to sue Wise. By the time of the judicial review hearing, Mr Delo had been provided with the personal data he was seeking but the High Court proceeded to consider the judicial review application based on public interest grounds. The High Court judge held that the Commissioner was not obliged to determine the merits of each and every complaint but had a discretion which he had exercised lawfully. He therefore dismissed the claim.

Mr Delo appealed to the Court of Appeal. The key questions on appeal were as follows:

1. is the Commissioner obliged to reach a definitive decision on the merits of each and every such complaint or does he have a discretion to decide that some other outcome is appropriate?
2. if the Commissioner has a discretion, did he nonetheless act unlawfully in this case by declining to investigate or determine the merits of the complaint made by Mr Delo?

Court of Appeal judgment

The court held that the Commissioner is not obliged to reach a definitive decision on the merits of each and every complaint. The wording in the UK General Data Protection Regulation (UK GDPR) does not say that the Commissioner must adjudicate, decide, determine, rule upon, or resolve a complaint, or that the complaints must be "upheld" or not upheld by the Commissioner. Rather, the wording is that the Commissioner must "investigate the subject-matter of the complaint" "to the extent appropriate", and then "inform" the complainant of the "progress" of the complaint and its investigation and its "outcome". The Court held that the meaning of "outcome" is broader than a conclusive determination or ruling on the merits. On the facts of this case, the Commissioner's decision that the conduct complained of was "likely" to be compliant with the UK GDPR was a relevant "outcome".

In relation to the second question, the court held that this was essentially an irrationality challenge. The court found that the High Court had not applied the wrong legal test therefore its application of law to the facts could not be impeached.

ICO orders employers to stop using facial recognition technology to monitor attendance of their employees

The ICO has issued enforcement notices ordering various leisure centre businesses to stop using facial recognition technology (FRT) and finger print scanning to monitor the attendance of its staff for the purposes of determining pay. The organisations had not shown why it was necessary or proportionate to use FRT and finger print scanning when there were less intrusive tools available such as ID cards or fobs, and the employers had failed to demonstrate why these less intrusive methods were not appropriate.

The organisations should have offered these less intrusive means proactively to employees. Given the imbalance of bargaining power in employment relationships, it was unlikely that the employees would feel confident refusing consent to their employers using their biometric data for attendance purposes.

The enforcement notices require the organisations to stop, within three months, from all processing of biometric data for monitoring employees' attendance at work, and to also destroy all biometric data that they are not legally entitled to retain.

Authors



Julia Wilson

Partner
London
+44 20 7919 1357
julia.wilson@bakermckenzie.com



Mandy Li

Knowledge Lawyer
London
+44 20 7919 1033
mandy.li@bakermckenzie.com

Regulations, consultations and guidance

ICO Draft Guidance – Recruitment and selection

As part of the UK Information Commissioner Office's (ICO) drive to update its regulatory guidance on various employment practices, it released draft guidance on data protection compliance with respect to recruitment practices in December 2023. The draft guidance is intended to provide practical guidance regarding matters such as automated decision-making and profiling, verifying candidate information, and keeping recruitment records. The consultation closes on 5 March 2024.

Some key points from the draft guidance include:

- **Legitimate interests assessment** – The ICO expects employers to carry out a legitimate interests assessment when relying on its legitimate interests as its lawful basis for recruitment activity. As this is likely to be the most appropriate lawful basis to rely on for most recruitment processes, this could mean employers may be expected to undertake an additional compliance measure for even "ordinary" recruitment activity.
- **AI-empowered recruitment tools** – Where employers use AI tools to make solely or partly automated recruitment decisions, a data protection impact assessment must be undertaken setting out why use of the tool is necessary and proportionate, whether a less intrusive alternative is available and how discrimination, accuracy and security risks are addressed. Measures employers can take to mitigate the risk include explaining the criteria against which the tool is making its assessment and providing an opportunity for candidates to challenge an automated decision.
- **Direct marketing** – Where employers or recruiters send potential candidates adverts for a job the candidate has not applied to (i.e., via email or LinkedIn), the ICO expects employers to comply with direct marketing laws. This may have significant implications for head-hunters and others in the recruitment industry who may routinely send unsolicited messages to potential candidates with respect to job opportunities.
- **Background checks** – Employers must ensure that the type of background check it wishes to perform is proportionate to an identified risk with respect to the role concerned. That means checks of an intrusive nature (e.g., criminal or social media checks) are unlikely to be lawful if routinely carried out across all roles within an organisation. This may mean employers will need to assess their background check procedures to ensure they align with the ICO's expectations.
- **Social media checks** – Checking a candidate's public social media profile is only lawful if it is necessary and proportionate in light of the specific role. The ICO expects employers to document the specific risks which the social media checks are intended to address and candidates should be given an opportunity to explain or comment on the employer's findings if necessary. Given social media checks have become common practice for many employers, documenting why such checks are necessary will be an important compliance step for such employers.

It remains to be seen how much the draft guidance will change following consultation. However, employers should be preparing to review their recruitment practices to ensure they comply with privacy law once the final guidance is published.

Author



Bobby Sarkodee-Adoo

Senior Associate

London

+44 20 7919 1752

[bobby.sarkodee-adoo](mailto:bobby.sarkodee-adoo@bakermckenzie.com)

[@bakermckenzie.com](mailto:bobby.sarkodee-adoo@bakermckenzie.com)

ICO Draft Guidance – Keeping employment records

The ICO is consulting on draft guidance which aims to provide employers with practical guidance on keeping employment records in compliance with their obligations under data protection law and give workers guidance on their rights regarding accessing records. The consultation closes on 5 March 2024.

Although the guidance refers to 'worker' and 'former worker', the scope is intended to cover all employment relationships therefore data relating to employees, contractors, volunteers, gig and platform workers. The guidance also uses the following terminology to set out the differences between legal obligations and good practice recommendations:

- **"Must"** – refers to legislative requirements
- **"Should"** – does not refer to a legislative requirement, but is something that the ICO expects you to do to comply effectively with the law. The guidance states that you should do this unless there is a good reason not to, and if you choose to adopt a different approach, you must be prepared to demonstrate that this approach complies with the law.
- **"Could"** – refers to an option or example that you could consider to help you to comply effectively. However, there are likely to be various other ways you could comply.

The guidance covers:

- The kinds of records employers can keep on their workers
- Lawful processing of workers' personal information
- Relying on a worker's consent
- Lawful bases for processing employment records
- Conditions for processing special category information
- How much personal information employers can hold
- How to keep workers' personal information accurate and up to date
- How long employers can keep workers' personal information
- What employers need to tell workers when processing their personal information
- Workers' rights to access employment records
- Workers' rights to have employment records erased
- Identifying who is responsible for data protection and employment records in the organisation

The guidance does not say anything particularly new, but it does offer practical and accessible guidance for employers – in particular, on the lawful bases for processing employment records. It explains the difficulty with relying on consent in an employment context given the difference in bargaining power between the parties and the ability for an individual to withdraw their consent at any time. The lawful bases that the ICO considers to be most relevant in an employment records context are:

- **Contract** – which is most likely to apply when employers need to collect and use information about workers under an employment contract. This lawful basis can only be used once an offer of employment has been accepted. *E.g., keeping records of worker names, addresses and salary information to meet the contractual obligation to pay them.*
- **Legal obligation** – which can be relied on when employers need to use personal information kept in employment records to comply with a common law or statutory

obligation. *E.g., To comply with the obligation to share workers' names, addresses and salary details with HMRC for tax purposes.*

- **Legitimate interests** – which may apply if keeping records of workers' personal information is necessary for an employer's legitimate interests or those of a third party. These legitimate interests will have to be weighed against protection of the workers' personal information. *E.g., Requesting references containing personal information about a job applicant from a previous employer.*

If you are keeping records of special category data, e.g., data containing information about the workers' racial / ethnic origin, or religious / philosophical belief, or health etc, then you will also need to identify a special category condition. The guidance sets out the following as most likely to be relevant in this context:

- **Employment, social security and social protection law** – noting that this does *not* cover records kept to meet purely contractual rights or obligations.
- **Legal claims or judicial acts** – this covers situations where the data is necessary to establish, exercise or defend legal claims. *E.g., where a worker has brought a claim against their employer.*
- **Substantial public interest** – the most likely substantial public interest conditions in this context are statutory and government purposes, equality of opportunity or treatment, racial and ethnic diversity at senior levels, preventing or detecting unlawful acts, regulatory requirements, preventing fraud, safeguarding of children and individuals at risk and occupational pensions.

Although the draft guidance may change following consultation, it is still a useful reference guide for employers reviewing their employment records policies or considering collating new categories of employee data.

Author



Jess Bowden
Associate
London
+44 20 7919 1214
jess.bowden@bakermckenzie.com

European Union



In the courts

Data subject access rights mean access to medical records should be free of charge

In brief

The European Court of Justice ruled that the data subject access rights under the GDPR meant that a patient was entitled to a copy of his medical records free of charge notwithstanding conflicting German federal law which required payment of a fee. Although this decision relates to medical law, it is transferable to other areas of law and employment law in particular.

Facts

A patient requested a copy of his medical records in order to check for potential medical liability claims. German federal law requires that a patient must pay a fee to access their medical records. This potentially conflicts with the data subject access request requirements (DSAR) of the GDPR which, broadly, require that a data subject is provided with information in response to a DSAR free of charge except in specified cases. The two lower courts ruled in favor of the patient and justified this by interpreting German law in accordance with EU law.

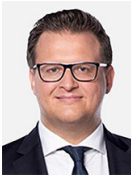
The Federal Court of Justice (Bundesgerichtshof, BGH) referred the issue to the European Court of Justice (ECJ) which ruled as follows:

- the GDPR requires a controller to provide the data subject with a first copy of their personal data free of charge. The right of access does not apply only in order to verify the lawfulness of processing and the data subject's motive for submitting the DSAR is irrelevant. Where a request is "manifestly unfounded" or "excessive" (for example where there are repeat and frequent requests for information) this could amount to an abuse of rights justifying a controller's refusal to respond or to charge a reasonable fee in the relevant circumstances;
- the provisions of the GDPR that permit member states to deviate from certain obligations and rights in national legislation do not apply to the right of access to personal data free of charge;
- the controller must provide an accurate and comprehensive reproduction of all personal data that has been processed; in this case for example the patient had the right to receive a complete copy of the documents contained in the medical records if this was necessary to enable him to verify the accuracy and completeness of the data held.

Comment

This judgment fits seamlessly into the case law of the ECJ, which has so far been very favorable towards the data subject. It also has a clear message for employment law practice; a request for information cannot be rejected nor considered an abuse of rights simply because the reason for the request is other than for verifying the lawfulness of data processing. Applied to employment law, this ruling shows that a DSAR is an admissible bargaining tool in dismissal protection proceedings provided it does not amount to an abuse of rights.

Authors



Christian Koops

Partner
Munich
+49 89 5 52 38 147
christian.koops@bakermckenzie.com



Matthias Koehler

Partner
Berlin
+49 30 2 20 02 81 662
matthias.koehler@bakermckenzie.com



Philipp Schlotthauer

Associate
Munich
+49 89 5523 8310
philipp.schlotthauer@bakermckenzie.com

Germany



In the courts

No entitlement to compensation for late and incomplete response to DSAR

In brief

The Regional Labor Court of Düsseldorf decided that an employer's late and incomplete response to a data subject access request (DSAR) did not entitle the data subject to non-material damages under the GDPR because the right to compensation arises only where unlawful data processing has taken place. While failure to respond to a DSAR in accordance with the GDPR is a breach of the legislation, it does not in itself amount to unlawful processing.

Facts

Broadly, the GDPR requires that information in response to a DSAR is provided to the data subject without undue delay and in any event within one month of receipt of the request (although this may be extended in relevant cases).

In a case decided by the Regional Labor Court, a customer service employee sent a DSAR to their employer on 1 October 2022 requesting that the employer respond with the information by 16 October 2022. The employer did not provide the information on time and initially provided incomplete information. Full information was not provided until 1 December 2022, i.e., approximately six weeks after the date requested by the employee and one month after expiry of the time limit prescribed by the GDPR.

The employee's claim for compensation under the GDPR was initially successful before the Duisburg Labor Court which awarded him EUR 10,000. However, the Regional Labor Court of Düsseldorf later overturned that decision on the basis that entitlement to compensation under the GDPR arises only where unlawful data processing has taken place. While the delayed and incomplete provision of information amounts to a breach of the GDPR, it does not constitute unlawful data processing. The Court also rejected the employee's argument that loss of control over his personal data as a result of the employer's failure to provide the requested information was sufficient to amount to unlawful data processing.

Comment

Providing information in response to a DSAR is a recurring issue in labor and data protection law consulting practice. Employers constantly have to process large amounts of their employees' personal data. The timely and proper provision of information to employees can therefore cause difficulties. As employee DSAR claims have become quite popular in legal proceedings and impose an additional burden on employers, the judgment of the Regional Labor Court could limit employees' leverage in settlement negotiations.

Looking ahead, however, the Regional Labor Court's decision could be overturned. Although the reasons for the decision have not been published, the Regional Labor Court could have been influenced by the recitals to the GDPR. The recitals to EU legislation set out the reasons for the main operative provisions; they are not legally binding but can be used by the courts to assist with interpretation. In the GDPR the recitals and the operative provisions that relate to entitlement to damages are inconsistent. The recitals suggest that entitlement arises as a result of processing that infringes the GDPR while the operative provisions effectively provide that the right arises in relation to any infringement of the legislation.

It remains to be seen how the courts will resolve this question going forward. Despite the decision of the Regional Labor Court, employers should continue to respond to DSARs as required by the GDPR. This is not only because of the potential for awards of compensation, but also the reputational risks attached to withholding information to which an employee is arguably entitled as well as the potential for complaints to the relevant supervisory authority for data protection.

LAG Düsseldorf November 28, 2023 - 3 Sa 285/23

Lack of independence justified removal of works council chair as data protection officer

In brief

The German Federal Labor Court (Bundesarbeitsgericht, BAG) has ruled that an employer was entitled to remove a works council chair as data protection officer (DPO) because the duties and responsibilities of the two positions were incompatible. In the circumstances of this case, the influential position of the works council chair on decisions that involved processing personal data compromised the independence necessary for the DPO to fulfil their compliance responsibilities.

Facts

Although in this case the BAG's decision was based on the pre-GDPR German Federal Data Protection Act (BDSG), under both legal frameworks the removal of the DPO requires good cause. The GDPR provides that a DPO should be in a position to perform their duties and tasks in an independent manner. A conflict of interest might justify removal of a DPO but the European Court of Justice (ECJ) has ruled that the extent to which such a conflict of interest exists should be decided by a national court on a case-by-case basis, taking into account all relevant circumstances. These include the organizational structure of the controller or processor and all applicable legal provisions and any other internal rules.

Although the Works Constitution Act imposes certain limits on data processing, a works council still has considerable leeway in deciding what personal data it holds and how it is processed. In this case, the works council chair had control and influence over works council data processing decisions. His role as DPO required him to scrutinize and enforce data protection compliance across the organization. The BAG decided that it was not feasible for him to hold both offices without there being a clear conflict of interest. Potentially he was policing decisions in which he had been personally involved which clearly compromised the independence of the DPO role. In this case, removal of the works council chair as DPO was justified. The BAG emphasized, however, that not every conflict of interest would be sufficient to justify removal or call into question the independence of a DPO.

Comment

In its decision, the BAG intentionally left open whether the office of a mere works council member is also in conflict with the function of DPO. So far, the BAG has consistently rejected this. Either way, because of many unresolved legal questions, we advise against appointing an employee to the position and rely on using an external DPO.

BAG - 9 AZR 383/19

Authors



Christian Koops

Partner
Munich
+49 89 5 52 38 147
christian.koops@bakermckenzie.com



Matthias Koehler

Partner
Berlin
+49 30 2 20 02 81 662
matthias.koehler@bakermckenzie.com



Philipp Schlotthauer

Associate
Munich
+49 89 5523 8310
philipp.schlotthauer@bakermckenzie.com

Spain



Regulations, consultations and guidance

Increased risks with using biometric data in monitoring workplace access and working hours

In brief

The widespread use by employers of certain technologies for HR purposes increasingly exposes them not only to financial penalties by the AEPD, the Spanish supervisory data protection authority, but also to possible claims by employees for breach of their fundamental rights.

Although processing biometric data (such as facial recognition, fingerprint recognition or eye recognition, etc.) had already been restricted in Spain for some time, at the end of 2023 the AEPD toughened its stance on employers' use of such technology for monitoring workplace access and working hours.

Key facts

In November last year the AEPD published its new guide on using biometric data for time and attendance control in which it severely limited the general use of these technologies for work purposes. This was a change from a previously more permissive approach to regulation in this area.

Broadly, biometric data is special category data; processing this requires greater levels of protection under the GDPR and the AEPD has now made clear that it considers processing of such data for time and access control to be high risk and generally disproportionate. In its view, general use of these technologies in the employment relationship is permissible only where specifically authorized by national legislation or in a relevant collective bargaining agreement. At the moment there is no legislation giving the authorization envisaged by the AEPD and collective bargaining agreements regulating this issue are very rare.

The more restrictive approach of the AEPD is consistent with recent decisions by the Spanish labor courts. In September, 2023, for example, the Labor Court of Alicante ordered a company to pay an employee compensation for breach of fundamental rights where it had used facial recognition technology without complying with the requirements of the GDPR.

Comment

This tougher stance by both the courts and the AEPD is likely to influence future decisions of the courts where biometric data is used for monitoring workforce activities and employers should be aware of the increased risks associated with these technologies in terms of fines and litigation. As these technologies are usually implemented for the entire workforce rather than simply one or two individuals, this could potentially give rise to multiple claims and significant financial liability.

In practice, collective bargaining agreements seem to be the most feasible way to regulate the use of these technologies going forward. Even where terms can be agreed, however, an employer could still be exposed to fines by the AEPD and claims by employees and/or trade unions in relation to historic use of biometric data.

[Guía sobre tratamientos de control de presencia mediante sistemas biométricos](#)

[Labor Court of Alicante Ruling 190/2023](#)

Authors



Marc Cucarella
Team Director
Barcelona
+34 93 2060861
marc.cucarella@bakermckenzie.com



David Molina
Senior Associate
Barcelona
+34 93 2551103
david.molina@bakermckenzie.com

Switzerland



Regulations, consultations and guidance

A quick look at recent changes to the data protection regime in Switzerland

In brief

Having been under review for several years, the Swiss Federal Act on Data Protection (FADP) and the Ordinance to the Federal Act on Data Protection (the Ordinance) came into effect on 1 September 2023. The revised FADP aims to ensure compatibility with EU law and introduces significant new changes.

In January, 2024 the European Commission confirmed the adequacy of the Swiss level of data protection so that cross-border data transfers continue to be possible without additional requirements.

The principal changes

Much like the GDPR, the FADP and the Ordinance now provide amongst others for specific governance obligations. The most important changes include the following:

- Data controllers must maintain a register of their processing activities similar to that required under the GDPR where:
 - they have more than 250 employees; or
 - they process personal data in a manner that poses risks to the rights of the data subjects concerned.
- Controllers have a duty to report data security breaches to the Federal Data Protection and Information Commissioner (FDPIC), while processors have a corresponding duty to inform the controller. Note that the threshold for security breaches which need to be notified under the GDPR is lower than the one under the FADP. In addition, controllers have a duty to inform the data subjects affected by a data security breach if the FDPIC requires this or it is necessary for the data subjects' protection and no exception from such information obligation applies.
- A controller has, under certain circumstances, an obligation to carry out data protection impact assessments.
- A processor may now only transfer personal data to a sub-processor with the prior consent of the controller; this consent can be general in scope provided the controller is informed in advance of any changes and has a right to object.
- In addition, data subjects must now be informed of any data processing (general notification obligation) — not only if sensitive data is being processed as was previously the case.
- The FADP also moved closer to the GDPR by no longer protecting the data of legal persons such as corporate entities, but only of natural persons.
- The FADP now explicitly provides for an extraterritorial scope.
- Foreign companies that process the personal data of data subjects in Switzerland on a large scale must provide a representative in Switzerland.

- Compared to the previous legislation, penalty provisions have been adapted under the FADP and the fines have been increased rather steeply from previously CHF 10,000 to a maximum of CHF 250,000. Unlike under the GDPR, fines under the FADP continue to target the responsible employees - and not the company itself.

Authors



Christoph Stutz
Partner
Zurich
+41 44 384 18 71
christoph.stutz@bakermckenzie.com



Johanna Moesch
Associate
Zurich
+41 44 384 13 38
johanna.moesch@bakermckenzie.com

Saudi Arabia



Regulations, consultations and guidance

New personal data protection law in Saudi Arabia: HR privacy considerations

In brief

On 14 September 2023, the Personal Data Protection Law (the PDPL) came into effect in the Kingdom of Saudi Arabia. Prior to this, there was no standalone personal data protection law in Saudi Arabia. Data privacy rights and protections existed only in the form of Shari'ah principles and certain discrete provisions in laws, regulations and other legal sources. The PDPL is a significant development in Saudi Arabia's legislative landscape that will have implications for almost all entities operating in the market or who offer their services to Saudi customers.

What is the PDPL?

Similar to other data protection regimes, such as the GDPR in the European Union, the overarching purpose of the PDPL is to ensure that the processing of all information (or data) relating to an individual (the data subject), regardless of its form, that would allow the individual to be identified, whether directly or indirectly, satisfies certain mandatory requirements to ensure the individual's rights of privacy are protected. For the purposes of the PDPL, "*processing*" is defined broadly as taking any action with an individual's personal data and includes collection, storage, modification, dissemination and transmission.

The PDPL will regulate both processing:

- that takes place in Saudi Arabia; and
- outside of Saudi Arabia, where it involves the personal data of a Saudi resident (i.e., by a controller situated outside of the Kingdom).

For the purposes of the PDPL, the Saudi Data and AI Authority (SDAIA) will be the competent authority responsible for enforcing the relevant legal requirements for a period of two years after it comes into force, but it may thereafter transfer this competency to the National Data Management Office (NDMO), a sub-division of SDAIA (hereinafter, we refer to the entity which exercises this competency as the Competent Authority).

Timeline for implementation

While the PDPL came into force on 14 September 2023, organizations have a period of 12 Hijri months to comply with the PDPL meaning there is effectively a 'grace period' until on or around 2 September 2024, during which no enforcement action should be taken in respect of non-compliance.

Different timelines may be applied to certain sector-specific entities, however and this will require businesses and organizations to remain vigilant in their efforts to ensure compliance with the PDPL to safeguard the privacy and security of an individual's personal information.

Key HR considerations

The PDPL imposes several obligations on controllers; we have included below an overview of a number of these new obligations, which may be of particular interest to a company's HR function:

- **Privacy policy**

Controllers must adopt a privacy policy and provide this to data subjects for review before collecting their personal data. The privacy policy must, at a minimum, specify:

- the purpose of the collection;
- the nature of the personal data to be collected;
- the collection and storage method and the means of processing;
- the manner by which the personal data will be destroyed; and
- the rights of data subjects, and details of how these can be exercised.

As such, HR will either want to consider the drafting or revising of current privacy policies to account for the new requirements.

- **Record of processing activities**

Under the PDPL, all organizations processing personal data, irrespective of size or industry, are obligated to establish a record of processing activities (ROPA). This comprehensive inventory details the organization's processing activities, including any HR-related processing, serving as a critical tool for compliance, transparency, and risk management.

Maintaining an accurate and up-to-date ROPA is paramount for ensuring PDPL compliance and safeguarding data subject privacy. Organizations will be expected to provide such ROPA to the Competent Authority upon request.

- **Data protection officer**

Controllers, upon meeting specific criteria, must appoint or assign a person to be responsible for compliance with the PDPL, the data protection officer (DPO), who must have the necessary expertise in data protection and operate independently. HR will need to consider suitable candidates for this position and conduct appropriate screening procedures to ensure a suitable DPO is appointed. Where this is an internal hire, HR will need to consider what changes will be required in terms of employee duties, benefits, post-termination restrictions, etc.

- **Employee work sessions**

Controllers will be required to hold work sessions for their employees to familiarize them with the principles of the PDPL. Work sessions can either be in-person seminars, online sessions or webinars (provided the controller can document employee attendance at the sessions). HR will likely need to assist with the arrangement of such work sessions to ensure compliance. HR will also need to give consideration to an attendance framework at these sessions and the consequences of non-attendance by employees.

- **Employees' health data**

Sharing employees' health data (such as their health status, whether physical, mental, psychological, medical treatment or involvement with the health services) must be limited to the least possible number of employees and only to the extent necessary to provide the required health services. As such, HR will need to review sickness / absence policies and procedures currently in place to ensure the sharing of health data is limited when it comes to handling sickness and injury records, occupational health schemes, medical examinations, testing, and health monitoring. This also includes implementing technical and organizational measures that are adapted to safeguard the security of such sensitive data.

- **Retention and access to employment records**

Controllers should only retain employment records for as long as is strictly necessary for the purpose of the processing activity, and employees have a right to access any

personal data that the employer holds. HR will, therefore, be integral in ensuring employment data is retained in a secure manner or destroyed (which can be policed through regular audits by HR) and ensuring suitable procedures are in place for dealing with data subject requests.

▪ Penalties

The PDPL provides that the Competent Authority will establish a committee to consider alleged breaches and administer fines; this will consider the violations and impose a warning or fine, according to the type, gravity and impact of the violation committed. However, in addition to financial penalties, breaches of the PDPL may give rise to the following penalties:

- criminal sanctions;
- confiscation of funds earned in connection with any breach of the law; and
- publication of decisions in local newspapers or by any other proper means to highlight the failings of a particular company.

Accordingly, the confiscation of funds attained in connection with breaches of the PDPL may amount to a sum which will be incredibly difficult to calculate.

HR will, therefore, need to be vigilant for any potential breaches (or allegations of breaches) of the PDPL by employees. HR should ensure they implement processes and procedures to deal with non-compliance and seek to update any disciplinary policies to incorporate action that may be taken where it is found there are deliberate (or avoidable) breaches of the PDPL.

Comment

Although implementation is a journey, the compliance deadline will arrive quickly, and it is imperative organizations are ready and compliant in all aspects of their business, including in relation to their workforce. If they have not already done so, HR should start to consider and implement a roadmap to ensure compliance with the considerations addressed above.

Authors



Joanna Matthews-Taylor
Partner
Dubai
+971 4 542 1943
joanna.matthews-taylor@bakermckenzie.com



Mark Tedeschi
Associate
Dubai
+971 4 542 1991
mark.tedeschi@bakermckenzie.com



Maher Ghalloussi
Associate
Dubai
+971 4 542 1956
maher.ghalloussi@bakermckenzie.com

Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

bakermckenzie.com

© 2024 Baker & McKenzie LLP. All rights reserved. Baker & McKenzie LLP is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.